The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
3/24/2010

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Mozilla Firefox, Mozilla Thunderbird and Mozilla SeaMonkey applications which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. The Mozilla applications (Firefox and SeaMonkey) utilize the same framework to display application specific information (e.g. webpages, emails, chats).

These vulnerabilities may be exploited if a user visits a webpage or opens a malicious file specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Mozilla Firefox version 3.6
Mozilla Firefox versions 3.5.7 and earlier
Mozilla Firefox versions 3.0.17 and earlier
Mozilla SeaMonkey 2.0.2 and earlier
Mozilla Thunderbird 3.0.1 and earlier

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla SeaMonkey. These vulnerabilities could allow an attacker to take complete control of an affected system or steal cookie-based authentication credentials. Details of these vulnerabilities are as follows:

Mozilla Firefox WOFF Decoder Integer Overflow Remote Code Execution Vulnerability (MFSA 2010-08)
A remote code execution vulnerability exists in Mozilla Firefox 3.6 due to an integer overflow error in the WOFF decoder because of a font decompression routine. An attacker can exploit this by crafting a malicious webpage designed to exploit this issue and convincing a user to browse to the page. Successful exploits may allow an attacker to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will result in denial of service conditions.

Mozilla Firefox 'window.location' Same Origin Policy Security Bypass (MFSA 2010-10)
A security bypass vulnerability exists which allows the ‘window.location’ Javascript object to be overridden in the Firefox web browser. This may allow attackers to create a website designed to supersede the object and bypass security restrictions and certain access restrictions to access data or execute arbitrary script code in the browser of an unsuspecting user in the context of another site. This could be used to steal sensitive information or to launch other attacks.

Mozilla Firefox Asynchronous HTTP Authorization Prompt Information Disclosure Vulnerability (MFSA 2010-15)
An information disclosure vulnerability exists due to the way that Mozilla Firefox does not attach an asynchronous HTTP authorization prompt to the correct browser window or tab. An attacker could exploit this vulnerability by a user to visiting a malicious site followed by the user opening a trusted site in another tab or window. The attacker would then be able to craft a false authentication prompt that would pose as the trusted page’s authentication prompt. If the user provides their credentials into the attacker’s authentication page then the attacker will have the user’s credentials for the trusted site.

Mozilla Firefox 'multipart/x-mixed-replace' Image Remote Memory Corruption Vulnerability (MFSA 2010-09)
A remote memory-corruption vulnerability exists due to a use-after-free error in the libpr0n library. An attacker can use a specially crafted animation with bits-per-pixel changes received via the 'multipart/x-mixed-replace' mime to cause the browser to free and then reuse a memory pointer. This dangling pointer condition may lead to arbitrary code execution. Failed exploits may result in denial of service conditions.

Mozilla Firefox, Thunderbird, and SeaMonkey XUL Cache Pollution Vulnerability (MFSA 2010-14)

A vulnerability exists in Mozilla Products which could allow an attacker to pollute a user's XUL cache and change the appearance of the browser by using style attributes such as font size and color. This cache can later be accessed by the browser chrome, which includes window frames, menus, toolbars, and scroll bars for use in the user interface. An attacker can exploit this issue by crafting a malicious webpage and tempting a user to access it. When the page loads the malicious site will be able to modify style attribute settings.

Mozilla Firefox Security Bypass Vulnerability (MFSA 2010-13)
A security bypass vulnerability exists due to missing security restrictions when preloading images in Firefox 3.6. It is possible to specify protocols that are normally not allowed in a web page such as "file:". This includes internal schemes implemented by add-ons that might perform privileged actions resulting in something like a Cross-Site Request Forgery (CSRF) attack against the add-on.

Mozilla Firefox, Thunderbird, and SeaMonkey Script Injection Vulnerability (MFSA 2010-12)
This vulnerability was originally identified in MFSA 2007-19. A script injection vulnerability exists in the ‘addEventListener’ and ‘setTimeout’ functions. An attacker can exploit these functions by using them on a wrapped object to inject scripts into another website’s context. This may cause cross site scripting and cross domain attacks.

Mozilla Firefox, Thunderbird, and SeaMonkey Multiple Vulnerabilities May Cause Remote Code Execution (MFSA 2010-11)
Multiple vulnerabilities exist in the Firefox browser engine which may allow for remote attackers to crash the browser or execute arbitrary code in the context of the application.

The above vulnerabilities may be exploited if a user visits a webpage or opens a malicious file specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to Mozilla Firefox 3.6.2, 3.5.8, 3.0.18, Thunderbird 3.0.2, and SeaMonkey 2.0.3 immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/38918
http://www.securityfocus.com/bid/38921
http://www.securityfocus.com/bid/38920
http://www.securityfocus.com/bid/38919
http://www.securityfocus.com/bid/38298
http://www.securityfocus.com/bid/38922

Mozilla:
http://www.mozilla.org/security/announce/2010/mfsa2010-09.html
http://www.mozilla.org/security/announce/2010/mfsa2010-10.html
http://www.mozilla.org/security/announce/2010/mfsa2010-11.html
http://www.mozilla.org/security/announce/2010/mfsa2010-12.html
http://www.mozilla.org/security/announce/2010/mfsa2010-13.html
http://www.mozilla.org/security/announce/2010/mfsa2010-14.html
http://www.mozilla.org/security/announce/2010/mfsa2010-15.html
http://www.mozilla.org/security/announce/2010/mfsa2010-08.html
http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.2

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0172
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0169
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0168
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0171
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0167
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0166
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0165
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0170
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0164

Secunia:
http://secunia.com/advisories/38608/